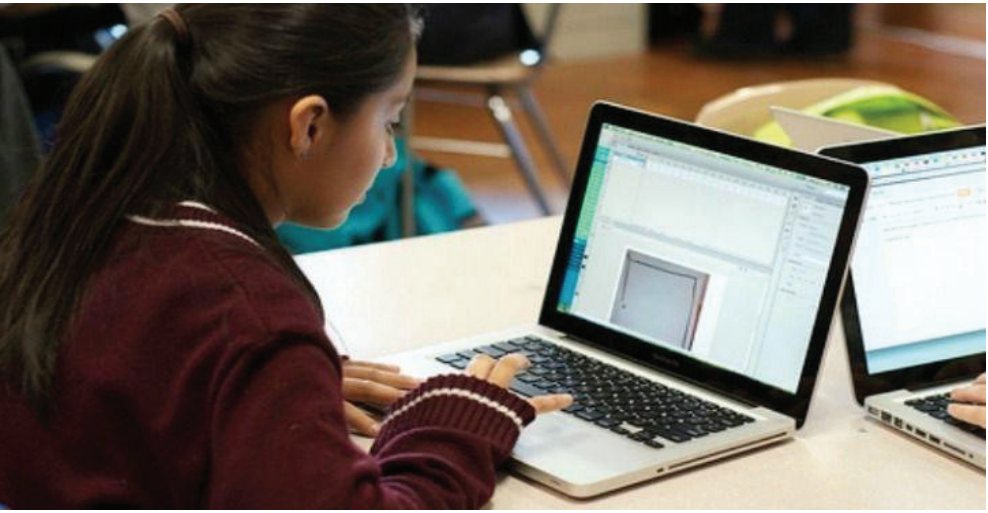
InfoSec for WOMEN

NATIONAL CYBER SECURITY AWARENESS MONTH

October, 2020

DESKTOP SECURITY



An unfortunate number of women are becoming victims of cyber crimes. The growing reach of the Internet and the rapid spread of information through mobile devices have presented new opportunities that could put some women at risk, so it is important to be mindful of the dangers.

A personal computer used without proper security measure could lead to exploiting the system for illegal activities using the resources of such in secured computers. These exploiters could be Virus, Trojans, Key loggers and sometimes real hackers. This may result in data theft, data loss, personal information disclosure, stealing of credentials like passwords etc. So, protect and secure your Personal Computer before it is compromised.

Browser Security

- Always update your Web Browser with latest patches.
- Use privacy or security settings which are inbuilt in the browser.
- Also use content filtering software.
- Always have Safe Search "ON" in Search Engine.

e-Mail Security

- Always use strong password for your email account.
- Always scan the email attachments with latest updated Anti-Virus and Anti-Spy ware before opening.
- Always remember to empty the Spam folder.

Wireless Security

- Change default Administrator passwords.
- Turn On WPA (Wi-Fi Protected Access) / WEP Encryption.
- Change default SSID.
- Enable MAC address filtering.
- Turn off your wireless network when not in use.

Modem Security

- Change the default passwords.
- Switch off when not in use.

Internet Security:

- Check the copyright issues before using the content of Internet. Follow Internet Ethics while browsing.
- Always access the site which uses https (Hyper Text Transfer Protocol Secure) while performing online transactions, downloads etc, which is secure.
- If the site uses SSL, verify the certificate details like who is the owner, expiry date of the certificate etc to confirm whether it is trusted or not. You can do this by clicking the lock icon.
- Use only original websites for downloading the files rather than third party websites.
- Scan the downloaded files with an updated Anti-Virus Software before using it.
- Install and properly configure a software firewall, to protect against malicious traffic.

Data Security

- Enable auto-updates of your operating system and update it regularly.
- Download Anti-Virus Software from a trusted website and install. Make sure it automatically gets updated with latest virus signatures.
- Download Anti-Spyware Software from a trusted website and install. Make sure it automatically updates with latest definitions.
- Use "Encryption" to secure your valuable information.
- Strong password should be used for "Admin" Account on computer and for other important applications like email client, financial applications (accounting etc).
- Backup: Periodically backup your computer data on CD / DVD or USB drive etc... In case it may get corrupted due to Hard Disk failures or when reinstalling/formatting the system.
- Recovery Disk: Always keep recovery disk supplied by Manufacturer / Vendor of the Computer System to recover the Operating System in the event of boot failures due to system changes such as uncertified Drivers/unknown Software publisher.
- Startup programs should be monitored / controlled for optimal system performance.

Don't leave your webcam connected:

There are too many apps capable of turning on your camera and slyly recording your movements without your knowledge. As a precaution disable camera permission and keep the lens of your camera closed or covered when not in use. Properly shutdown and switch off your personal computer after the use along with your external devices like Monitor, Modem, Speakers etc

Backup your data:

Backing up your data saves you when your computer crashes due to electrical outage or surge, like a lightning storm. It also helps if you fall prey to the newer type of ransomware, which encrypts your sensitive data. You can do your back-up manually by transferring important documents to an external hard drive.